

# Digital investigations in the Cloud



Cloud computing is the new hot topic. Although many see using and sharing software hosted on the Internet as a natural next step in our exploitation of the World Wide Web, it can however pose a challenge to those involved in digital forensics investigations. Reliance by organisations on third-party providers of 'Software as a Service' (SaaS), 'Platform as a Service' (PaaS) and 'Infrastructure as a Service' (IaaS) solutions can significantly hinder the ability of internal or external forensics specialists to conduct digital investigations. None of the associated problems are insurmountable – but effective solutions may require considerable work and time. This paper examines the practical steps needed to ensure investigations can progress unhindered. Also identified are potential issues, practical solutions and the tools required to investigate security breaches in the Cloud effectively.



**Neil Hare-Brown**  
Chief Executive Officer

**John Douglas**  
Technical Director



## Contents

<b>Introduction</b>	<b>1</b>
<b>Parting the clouds</b>	<b>2</b>
<b>Corporate investigations in the Cloud</b>	<b>3</b>
<b>Contractual support for investigations</b>	<b>4</b>
<b>Managing disclosure</b>	<b>5</b>
<b>Storm cloud on the horizon?</b>	<b>6</b>
<b>Cloud busting and crime fighting</b>	<b>7</b>
<b>Working towards silver linings</b>	<b>8</b>
<b>The forensic process</b>	<b>9</b>
<b>Conclusion</b>	<b>10</b>
<b>References</b>	<b>11</b>
<b>About QCC</b>	<b>12</b>
<b>The authors</b>	<b>13</b>

Thanks to  
**high-speed  
broadband**  
'the Cloud'  
is coming of age

# 1 Introduction

Cloud computing is a rebadge of services provided by SaaS/PaaS/IaaS companies, and encompasses the even older concept of an Application Service Provider (ASP). These organisations are referred to here as Cloud or Communications Service Providers (CSPs).

At this point it may be important to draw a distinction between true 'Cloud' services and 'managed' services. 'Managed' services are provided by a third party but are accessed by the customer over a private network (physical or virtual). Cloud services are accessed purely via the Internet. However, many of the challenges posed to successful digital investigations apply equally to both.

Many pundits proclaim a new dawn of outsourced services. Of course, many of them have vested interests in proclaiming their significance. However, there is no doubt that thanks to high-speed broadband 'the Cloud' is coming of age. Simply by going online, businesses and consumers can access either the services of their own organisation, or one of the many hundreds of thousands of services hosted by third parties – all via the Internet.

For a number of years now, online services such as Amazon and eBay have been household names. Although generally not referred to as Cloud applications, the functionality provided by these and similar services considerably outshines that of many corporate applications. Businesses also use these applications, finding that purchasing via such services can be quick and cost effective.

As these services move into the business space, they introduce security and investigatory issues (more about this later on).

The better-known Cloud/SaaS applications such as Salesforce.com, Microsoft and NetSuite are also widespread within businesses globally. In fact, they are actually not that different in terms of the potential risk that their use introduces and the associated complexities of managing data ownership and security.

Outsourcing computing power to save money and take advantage of other efficiencies has driven the PaaS and IaaS industry. GoogleApps and Heroku, now part of Salesforce.com, enable organisations to migrate their applications and databases outside of their corporate networks, while companies such as Rackspace, Amazon EC2 and GoGrid will take care of the hardware and storage components.

As one observer quipped: "So operating in the Cloud is like outsourcing all your IT services, except you don't know where your data is." A layman's observation that is perhaps not altogether inaccurate.

## 2 Parting the clouds

The way in which Cloud computing impacts on digital investigations varies greatly depending on the type of analysis needed. However, as you will read, most of this impact is procedural as opposed to technical.

In the civil and corporate arena it is largely possible to support digital investigations by specifying key requirements within supplier contracts. This is not a simple task but with the right amount of care and expertise it should be achievable. However, when digital forensics are needed to support criminal investigations, the problems introduced by Cloud computing become more severe.

As experienced digital investigators and forensics specialists, we at QCC have worked with corporate clients, CSPs and law enforcement agencies and officers. Over the past few years, we have noticed that more powerful and functional computing is generating ever greater evidential potential. However, some of the evidence is held 'server-side' within the Cloud. Our established relationships with CSPs enable us to provide a better service to our clients and all the parties involved in an investigation.

---

*Many investigations flounder because key technical staff and the management personnel needed to make decisions are simply not available.*

---

## 3 Corporate investigations in the Cloud

When it comes to the use of digital forensics in corporate investigations, pre-conditions that support successful analysis include the following:

- Well written supplier contracts that support not only the implementation and verification of adequate security measures, but also allow for investigatory actions.
- A good understanding by the Incident Management/Forensics Team of the technologies delivered by each CSP.
- Good, established (pre-incident) relationships between CSPs and corporate investigators and legal teams.
- Tested and effective incident response plans.

There are a whole host of security mechanisms that CSPs and their customers should consider. These must not only support the day-to-day requirements for confidentiality, integrity and availability of data hosted in the Cloud, and accountability for access to that data – but if implemented effectively will also significantly increase the chance of a successful digital forensic investigation.

Organisations such as the Cloud Security Alliance (CSA), the European Network and Information Security Agency (ENISA) and the International Systems Audit & Control Association (ISACA) have issued guidance in this area and the international standard for Information Security Management, ISO/IEC 27001 remains a great point of reference for good practice. There may be regulations such as Sarbanes-Oxley or PCI DSS that require the implementation of specific controls to protect data.

Here are a few examples of security, process and design control that will help digital investigations:

- **Logging and data retention/backups**  
Ensuring that these two important aspects of data management are coherently linked together maximises the information available in a complete chronology.

## 4 Contractual support for investigations

- **Use of virtualisation**  
Smart use of virtual machines will enable the rapid collection of data for analysis. The virtualisation design should be confirmed as being forensics friendly.
- **Documentation**  
Both summary and in-depth descriptions of code, configuration, interfaces and data flow within Cloud-hosted systems will assist investigators.
- **Technical support & senior management**  
Many investigations struggle because key technical staff and the management personnel needed to make decisions are simply not available. Ensure you know the 'who, what, when, where and how'.
- **Secure remote access**  
Such a service may often be vital when discovery and data carving activities are needed. Imaging and full acquisition are preferred but not always possible or practical.

As always, the best environment for digital forensics investigations in the Cloud is that which is established through good organisational control. Agreeing Standard Operating Procedures (SOPs) between the CSP and its customers is vital to ensuring investigations go unhindered, and can provide rapid and meaningful results. This is achieved by establishing effective contractual requirements between the CSP and its customers and by putting in place an ongoing programme of communications and exercises to ensure contractual adherence.

Unfortunately, this most fundamental requirement for effective investigations is often woefully lacking. CSP contracts hardly ever make reference to, let alone embrace, the potential need for cooperation in support of digital investigations.

This means that when an organisation needs to perform digital forensics as part of an investigation into a growing range of incidents including data theft, loss and other misuse, they have to rely purely on the goodwill and best efforts of the CSP. In many cases this has an adverse effect on the investigation. Damaging security breaches may continue needlessly, guilty parties may abscond or never be identified. Losses may be considerable and often unquantifiable – all for the want of a well-written contract.

We have undertaken many investigations where the Data Centre Manager simply is not ready, willing or able (unless with authority in triplicate from his CEO) to attend to the critical actions needed to support a digital investigation. On far too many occasions this has led to significant time being needlessly added to the investigation. It has also risked evidential artefacts being lost or damaged.

In addition, many CSPs simply do not have enough suitably knowledgeable staff to be able to assist an investigation team.

In many cases, evidence may not only be found in a customer's systems and data, but may also be identified in the many infrastructural systems that support the customer. These include firewalls, intrusion detection systems, email filters and event logs from a host of supporting systems. This metadata can often provide vital 'glue' in putting together a chronological timeline of events, as well as the creation, modification or deletion of evidential artefacts.

*The best environment for digital forensics investigations in the Cloud is that which is established through good organisational control.*

CSPs obviously want to provide standard contracts for their customers, be they small, medium or large enterprises. Many of the contracts that our legal specialists have reviewed are, in their opinion, significantly biased in favour of the CSP with regard to liability for both quality of service, and security.

This oversight gives the ethical and truly professional CSPs a chance to shine by offering their clients well-written contracts that embrace the need for security controls, cooperation and collaboration during investigations as an inherent part of their service provision, whilst still protecting their business as a supplier. Customers of Cloud-based services need to ensure that such contractual obligations are both offered and met. Of course, there is an obvious cost implication here which will impact the bottom line of one or both parties. But it is a cost worth bearing.

---

*Losses may be considerable and often unquantifiable – all for the want of a well-written contract.*

---

## 5 Managing disclosure

So far, we have discussed the relative ease with which corporate investigations should take place – as long as contracts, preparation, planning and communications hurdles are overcome. But there is another complication that sometimes occurs. This is the discovery and handling of forensic artefacts where some kind of disclosure must be made to the relevant authorities.

Examples of such discoveries include those relating to:

- Criminal activity (depending on the possible offences and jurisdiction)
- Incidents that must be disclosed to regulatory authorities, such as breaches of privacy related to the loss of, or unauthorised access to, Personally Identifiable Information (PII)
- Incidents which the organisation is contractually obligated to report to their customers or suppliers, e.g., Payment Card Industry Data Security Standard (PCI DSS) incidents

It is important to understand that if a third party client/partner/supplier (including the CSP) becomes aware of certain types of incident then they may also be duty bound to disclose them without the consent or knowledge of those involved. It would again be good practice to require this disclosure as part of a contractual obligation. Examples of such incidents involve the reporting of suspicious activity relating to money laundering, or the possession of unlawful material.

Before such discoveries are made it is important to know what your duties are with regard to required disclosure of personal or business data held by your CSP. Appropriate SOPs can then be prepared and applied when needed.

## 6 Storm cloud on the horizon?

When it comes to effective criminal investigation there are numerous barriers to successful Cloud-based digital forensics investigations by law enforcement agencies. Firstly, consider CSPs who deliver services internationally. The problem areas here are twofold:

- **Cross-jurisdictional issues**

It is generally not permissible for a law enforcement organisation and its appointed digital forensics specialists to access systems belonging to companies outside that agency's jurisdiction.

Where cross-jurisdictional and/or international agreements are in place, these generally require the organisation which has jurisdiction to appoint its own law enforcement and digital forensics specialists. These specialists then provide the results to the law enforcement agency which made the original request. Sometimes this data cannot be relied upon fully because of conflicting or non-existent operating standards.

- **Timescales**

Even when there are mechanisms by which law enforcement agencies may collaborate with regard to investigations requiring digital forensics, the bureaucracy involved to allow such collaboration is usually time consuming. Timescales are so long that the hope of recovering evidential artefacts diminishes substantially. This is exacerbated by the CSPs very short data and log retention policies (for operational reasons).

One area where national governments are now focussing is that of Data Retention (DR), although extended timescales here are largely aimed at supporting national law enforcement investigations. This is not particularly helpful when investigating criminal activity affecting Cloud services internationally.

Investigations by law enforcement officers involving international CSPs are not, therefore, straightforward. However, the problems are not insurmountable. This can be seen by those investigations undertaken by leading agencies such as the Serious Organised Crime Agency (SOCA) and the Police Central E-Crime Unit

(PCeU) in the UK, as well as the Federal Bureau of Investigation (FBI) in the United States and the Federal Security Service (FSB) in Russia. However, the level of criminality required for such agencies to mobilise is particularly high. As one would expect, the cost of these investigations is prohibitive when compared to the budgets for most digital forensic analysis.

Where investigations have no need to cross jurisdictional boundaries the situation becomes less complex, but here the problems increasingly lie in the following areas:

- **Obtaining warrants**

Law enforcement agencies must obtain warrants in order to access, seize/image and forensically analyse evidence in data stored at CSPs.

- **Time and cost**

Significant time and cost is added to the process not only for law enforcement agencies but also for the CSPs (for which they may not be well compensated, if at all).

- **Timescales**

The timescales for technical investigations will increase due to greater infrastructural complexity.

Considerations associated with the presentation of evidence may also add complexity and increase timescales and cost.

Although the likelihood of digital evidence being located in the Cloud is increasing, budgets for digital forensics are constantly being squeezed.

Now is not a good time for digital forensics in law enforcement investigations involving the Cloud because the costs for investigation are high. Ultimately it will be the victims of crime that will suffer – along with public perception of law enforcement effectiveness. The challenges for our international legislators are immense.

## 7 Cloud busting and crime fighting

For law enforcement agencies, their appointed digital forensics specialists and those that govern the jurisdictions concerned, there are significant hurdles to overcome. And CSPs need to be ready to respond to the increasing number of warrants and court orders granting access to their systems.

Ways must be found for law enforcement agencies to serve warrants internationally via their counterparts. This may involve multiple jurisdictions simultaneously. The cost issues here will be significant, although possibly overcome with careful use of technology, such as:

- Remote warrant execution and management through trusted agency counterparts
- Remote analysis tools operated under the supervision of a trusted domicile agency, including full audit trail of the analysts' actions
- Use of cryptographic digital signatures as well as confidential handling controls for evidential artefacts and the actions undertaken to acquire them

There are already fledgling technologies that may satisfy these points but they require an additional framework within which to function. This would include:

- Agreed international standards for digital forensics investigations.
- An agreed legislative trust for international warrant execution.

---

*Although the likelihood of digital evidence being located in the Cloud is increasing, budgets for digital forensics are constantly being squeezed.*

---

## 8 Working towards silver linings

In order for the corporate and government sectors to use Cloud services successfully, it is essential for contractual agreements to be drawn up properly with CSPs, enabling investigations to take place unhindered and efficiently.

Just as important is that the suitability of contracts is verified and agreed procedures are audited. Response plans for the company-appointed digital forensics investigators and each CSP should also be assessed. This level of governance will come with a price tag, which inexorably, will be built into the overall cost of Cloud computing.

For law enforcement agencies, the use of Cloud services by criminals is looking like the perfect storm.

Interesting developments in the areas of lawful interception and consequent data retention were highlighted in recent challenges against Blackberry manufacturer Research In Motion Ltd (RIM) by the governments of Saudi Arabia and India. Authorities in these two countries feel that access to communications is essential in their fight against international terrorism and organised crime.

The United States government has suggested that organisations processing RIM Blackberry communications must have an office in a US jurisdiction where an interception warrant can then be served and actioned.

It is certain that most executives of CSPs would reel at the costs of such a regulation being enforced. However, this proposal is undoubtedly an interesting approach to solving some of the problems mentioned earlier.

Understanding how governments and their law enforcement agencies seek to obtain intercepted data will enable mechanisms to be created that allow digital forensics to be performed more easily across jurisdictional boundaries. It is possible that law enforcement agencies such as Interpol will have an important role to play in this area.

## 9 The forensic process

The impact on traditional digital forensic techniques of conducting a Cloud-based investigation is not as significant as you might think. At QCC, we have been dealing with data centre-based examinations for years. It does come with its own set of interesting challenges, but by and large, these are well understood and relatively straightforward to deal with.

In all investigations, it is critical to be able to rely on every point of contact. If everyone involved carries out their responsibilities in a timely manner, the duration of the investigation may be curtailed and the outcome affected in a positive way.

Ensuring that the Data Centre Manager understands the nature of the investigation, along with ways in which they can help, is paramount. Preferably, this role should be predefined with the client in a three-way agreement long before any investigation is warranted.

A key consideration from a technical perspective is the distribution of data – both inside and outside the data centre itself. The use of clusters and virtual machines can make life harder and easier at the same time. Ideally, preservation of evidence is best achieved by isolating relevant systems. Can this be practically achieved? Moreover, is it planned for? This is where incident response planning can make all the difference – and often there may be a commonality between planning for both investigations and business continuity.

The issue of proportionality is a current focus of civil courts. This means that only data pertinent to the investigation should be captured.

Much of the concern around proportionality stems from data protection issues and the potential electronic discovery requirements which may arise after data capture. Careful planning and understanding of the relevant laws is a prerequisite.

## 10 Conclusion

For those taking advantage of the Cloud computing in their business, enabling effective digital forensic investigations is not an impossible task. But it does require care and solid technical and legal support from specialists in the field.

Within law enforcement, the challenges are international both in nature and scale. The solutions may take many years to evolve before they become effective, with at least one high-profile international incident of non-collaboration an absolute certainty.

Preparation and planning – whether by international agreement, contract or tested operating procedures – will be critical if digital investigations and forensics in Cloud computing environments are to be both possible and practical. This will take effort, time and money.

The adoption of the Cloud by those wishing to commit crime and misuse systems and data for their own ends is already a growing trend. However, with the right tools, professional support and international legislation, law enforcement agencies may eventually prevail.

---

*Ensuring that the Data Centre Manager understands the nature of the investigation, along with ways in which they can help, is paramount.*

---

## 11 References

**Cloud Security Alliance (CSA):**

Security Guidance for Critical Areas of Focus in Cloud Computing v2.1  
<http://www.cloudsecurityalliance.org/csaguide.pdf>

**European Network and Information Security Agency (ENISA):**

Cloud Computing – Benefits, Risks and Recommendations for Information Security  
[http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at\\_download/fullReport](http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport)

**International Standards Organisation (ISO):**

ISO/IEC 27001 – International Standard for Information Security Management  
[http://www.iso.org/iso/catalogue\\_detail?csnumber=42103](http://www.iso.org/iso/catalogue_detail?csnumber=42103)

**Information Security Incident Management:**

A Methodology  
<http://shop.bsigroup.com/en/ProductDetail/?pid=00000000030165302>

---

*Preparation and planning  
will be critical if digital  
investigations and forensics  
in Cloud computing  
environments are to be both  
possible and practical.*

---

## 12 About QCC

QCC Information Security is a dedicated team of specialists in Digital Forensics and Cyber Security Investigations.

Formed in 1996 by ex-officers of the UK Metropolitan Police Computer Crime Unit (CCU) and Technical Support Unit (TSU), their work has produced many tools and publications to assist the Digital Forensics investigator.

We work for law enforcement, government and commercial organisations investigating a range of incidents and cases. We are also accredited by Visa and MasterCard as Qualified Forensics Investigators (QFI).

QCC has designed the Blackthorn governance, risk and compliance system for management of incidents, cases, assessments, audits and any other security activity.

## 13 The authors

**Neil Hare-Brown** is CEO of QCC. He has over twenty-five years of experience in information security, risk assessment and digital investigations and in 2007 published a book on Incident Response published by British Standards (BIP: 0064).

Neil has an MSc in Information Security from Royal Holloway, University of London. He is a Certified Information Systems Auditor (CISA) and a Certified Information Systems Security Professional (CISSP).

He is a proud member of the Cloud Security Alliance and British Computer Society, as well as the City of London Company of Security Professionals.

**John Douglas** is a forensic specialist and has been involved in the forensic examination of various criminal and civil cases including indecent photographs of children, rape, harassment, fraud, abuse of privilege, murder, deception, immigration fraud, people trafficking, drugs, theft, forgery and many others. He holds an MSc in Forensic Science in the field of Forensic Computing from the Royal Military College of Science, Cranfield University.

John was awarded a Metropolitan Police Commanders Commendation in 2007 for his work in bringing to justice a dangerous predatory paedophile.

### Contact details

Neil Hare-Brown: [neilhb@qccis.com](mailto:neilhb@qccis.com)  
John Douglas: [johnd@qccis.com](mailto:johnd@qccis.com)



**QCC Information Security Ltd • Buchanan House  
24-30 Holborn • London EC1N 2LX • UK**

**Tel: +44 (0)20 7353 9000**

**Email: [contact@qccis.com](mailto:contact@qccis.com)**

**Web: [www.qccis.com](http://www.qccis.com)**

This publication is for general guidance only and information in it is subject to change without notice. Please contact QCC Information Security Ltd for latest information on QCC products and services. No part of this publication may be reproduced or transmitted, in any form or by any means, or stored in any retrieval system of any nature, without prior written permission of QCC Information Security Ltd, except for fair dealing under the Copyright, Designs and Patents Act.

© Copyright QCC Information Security Ltd. 2011. All Rights Reserved.

QCC-MKTG110112a-MS-White Paper Digital Investigations -v0.1